(12) UK Patent Application (19) GB (11) 2 332 548 (13) A

(43) Date of A Publication 23.06.1999

(21) Application No 9827361.8

(22) Date of Filing 11.12.1998

(30) Priority Data
(31) 9726828.8 (32) 20.12.1997 (33) GB
(31) 9816170.6 (32) 27.07.1998

(51) INT CL[6]
B60R 25/00 , E05B 49/00

(52) UK CL (Edition Q)
G4H HRBS HRCS HTG H1A H13D H14A H14B H14D H14G H60
U1S S1820

(56) Documents Cited
GB 2311155 A US 4209783 A

(58) Field of Search
UK CL (Edition Q) G4H HRCE HRCM HRCS HTG
INT CL[6] B60R , E05B , G07C

(71) Applicant(s)
Rover Group Limited
(Incorporated in the United Kingdom)
International Headquarters, Warwick Technology Park, WARWICK, CV34 6RG, United Kingdom

(72) Inventor(s)
Jeremy John Greenwood

(74) Agent and/or Address for Service
Alan S Wilson
Rover Group Limited, Gaydon Test Centre, Banbury Road, Lighthorne, Warwick, CV35 0RG, United Kingdom

(54) Abstract Title
Security system

(57) A security system suitable for a vehicle 10 comprises: a remote transponder 16, and a transmitter / receiver 14 which is mounted on the vehicle 10 and which is associated with a controller 12 for controlling the security functions of the vehicle 10 in response to a signal from the transmitter / receiver 14. The transponder 16 is arranged to transmit a security signal in one or more of a predetermined range of channels. The transmitter / receiver 14 is arranged to scan the range of channels and to determine in which one or more of those channels the security signal has been transmitted.

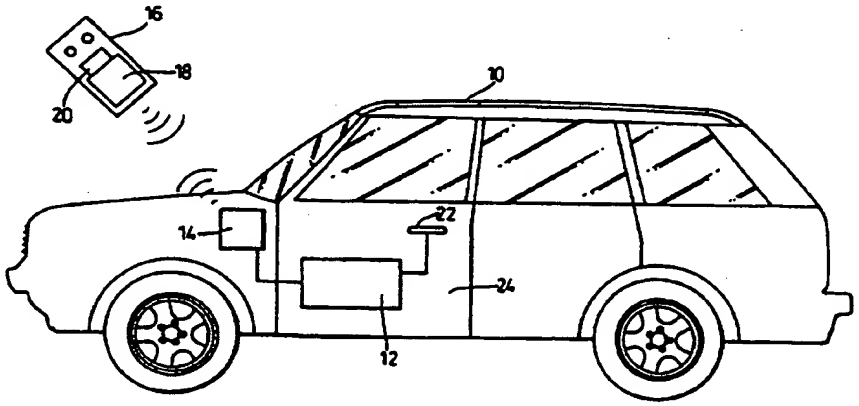


Fig. 1

GB 2 332 548 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

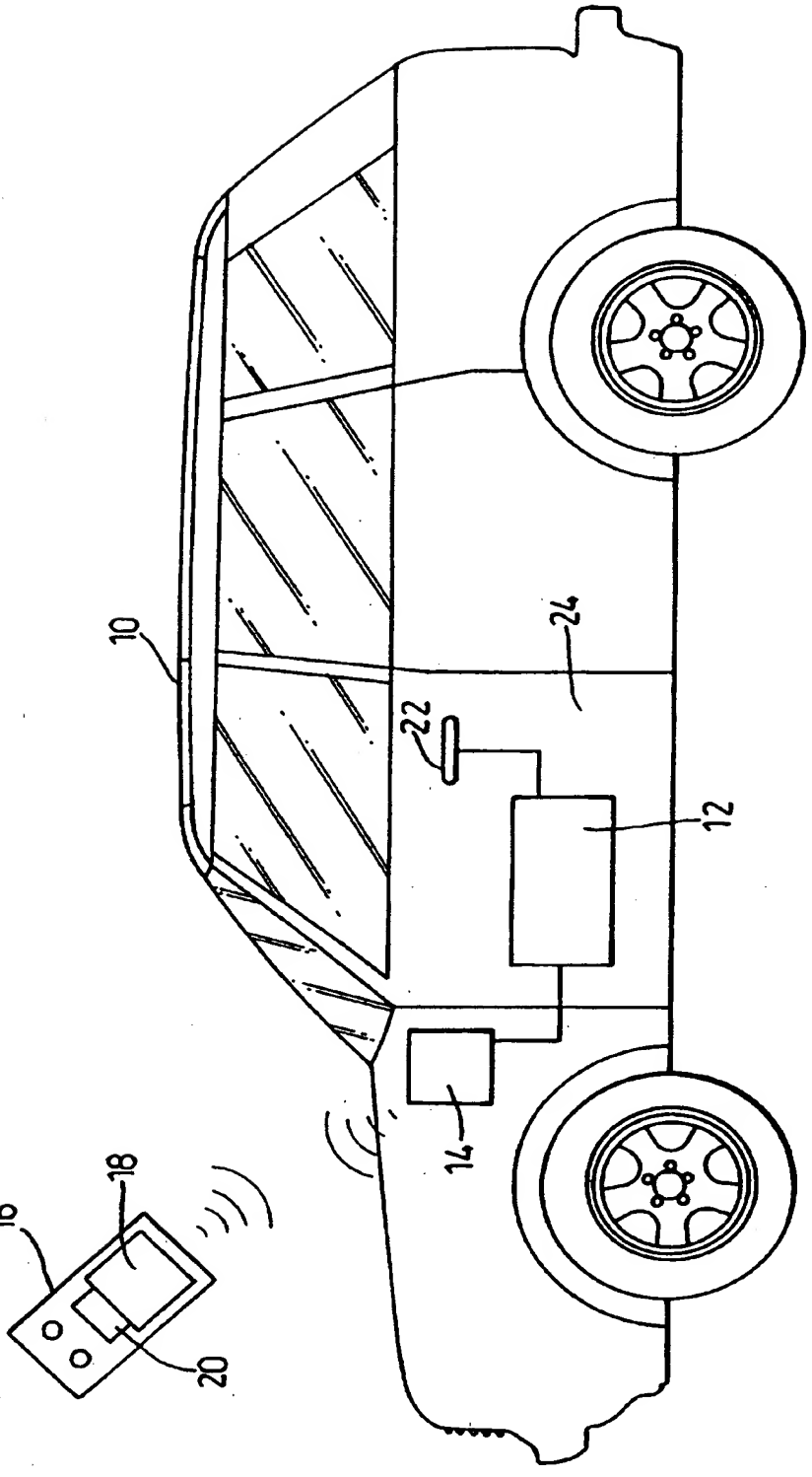
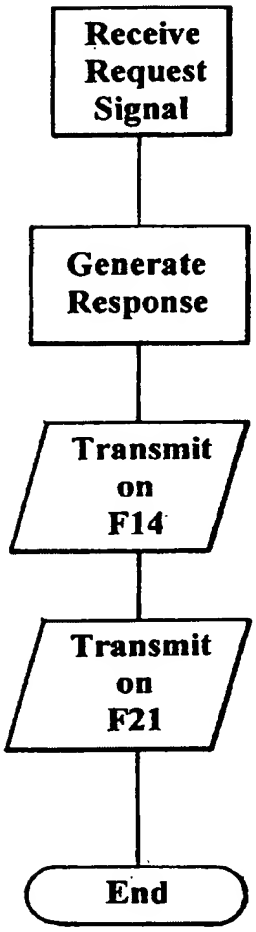


Fig. 1

Remote Transponder Operation



Security signal transmitted on channels 14 and 21

Fig. 2

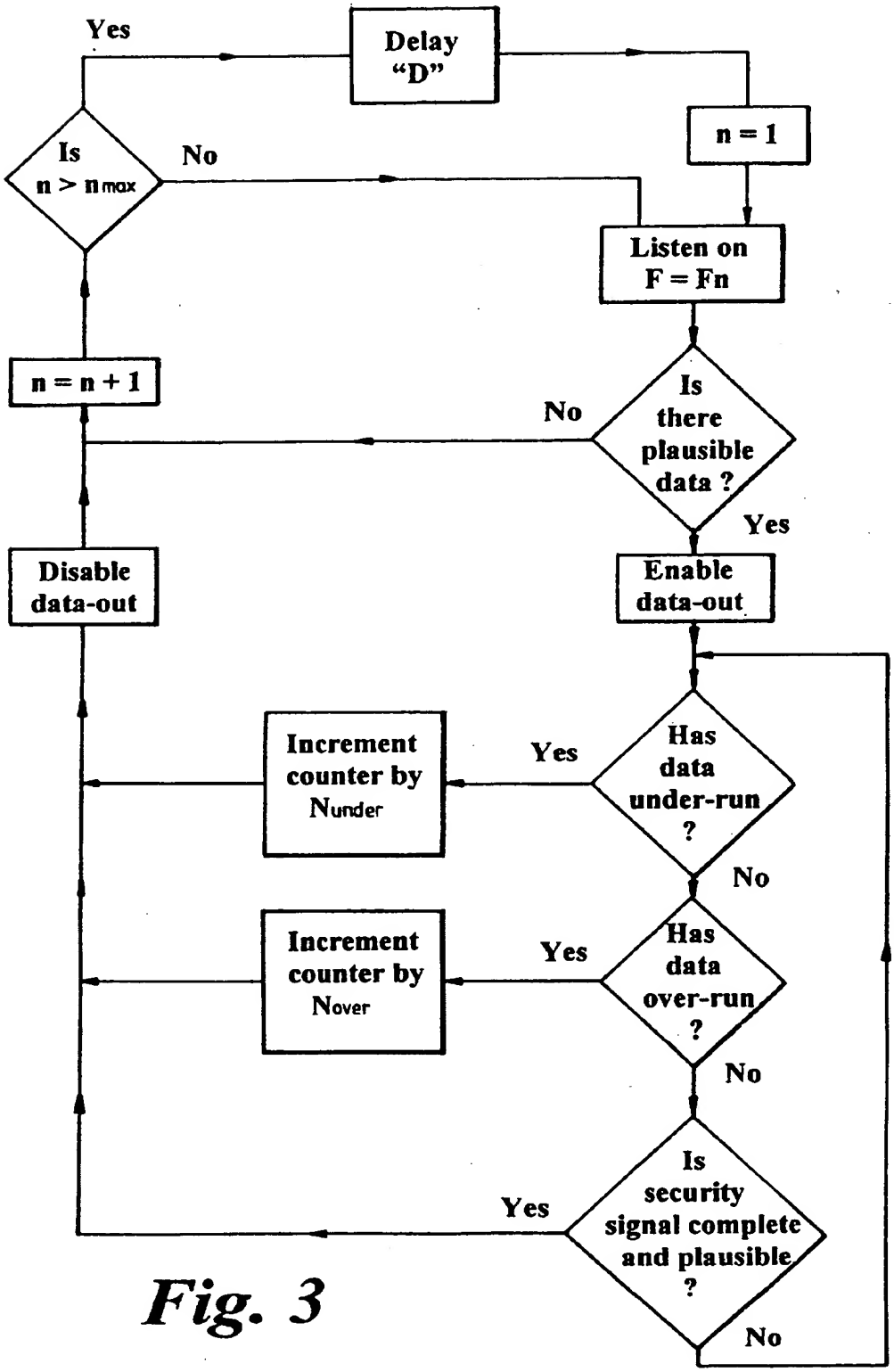

Yes
Delay "D"
n = 1
Is n > nmax
No
Listen on F = Fn
n = n + 1
No
Is there plausible data ?
Yes
Disable data-out
Enable data-out
Increment counter by Nunder
Yes
Has data under-run ?
No
Increment counter by Nover
Yes
Has data over-run ?
No
Is security signal complete and plausible ?
Yes
No

Fig. 3

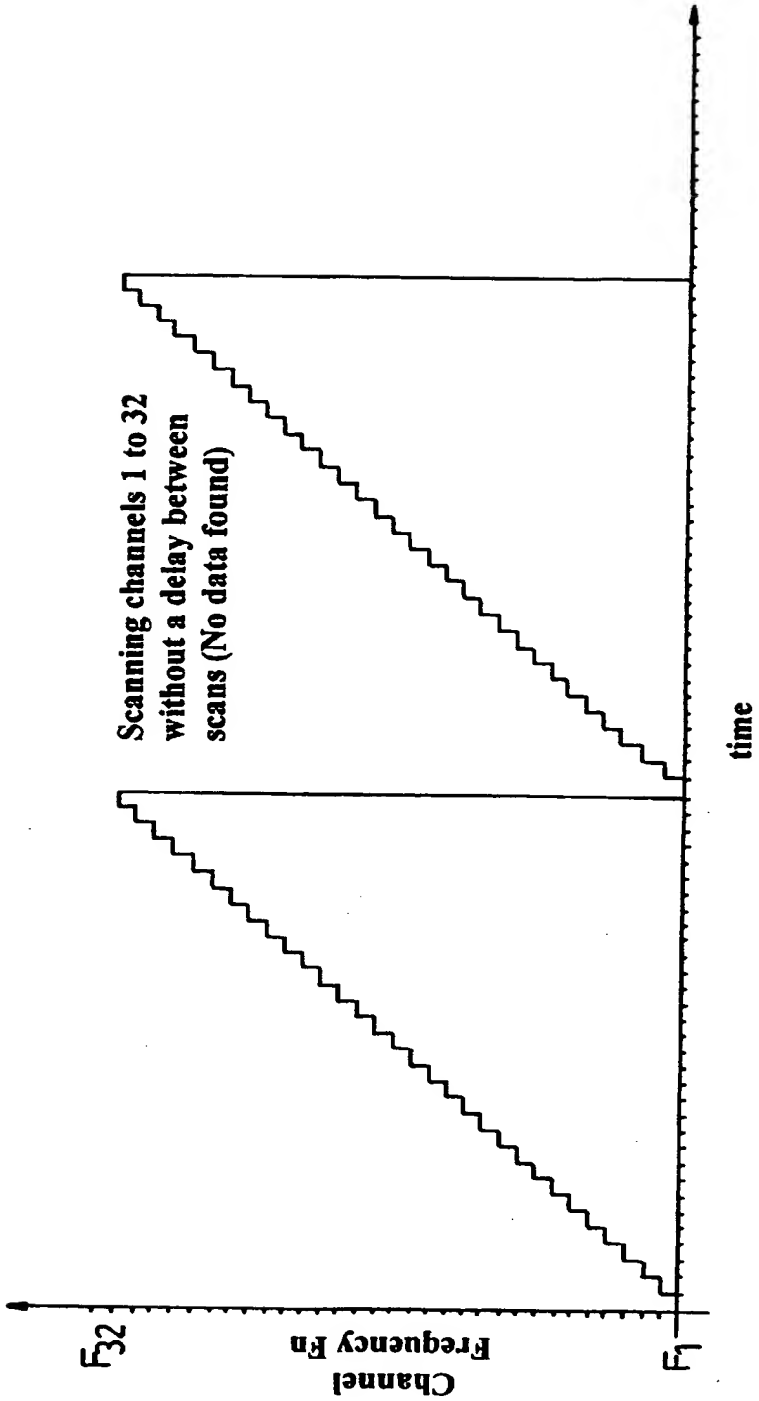

Scanning channels 1 to 32
without a delay between
scans (No data found)
time
Channel
Frequency Fn
F32
F1

Fig. 4a

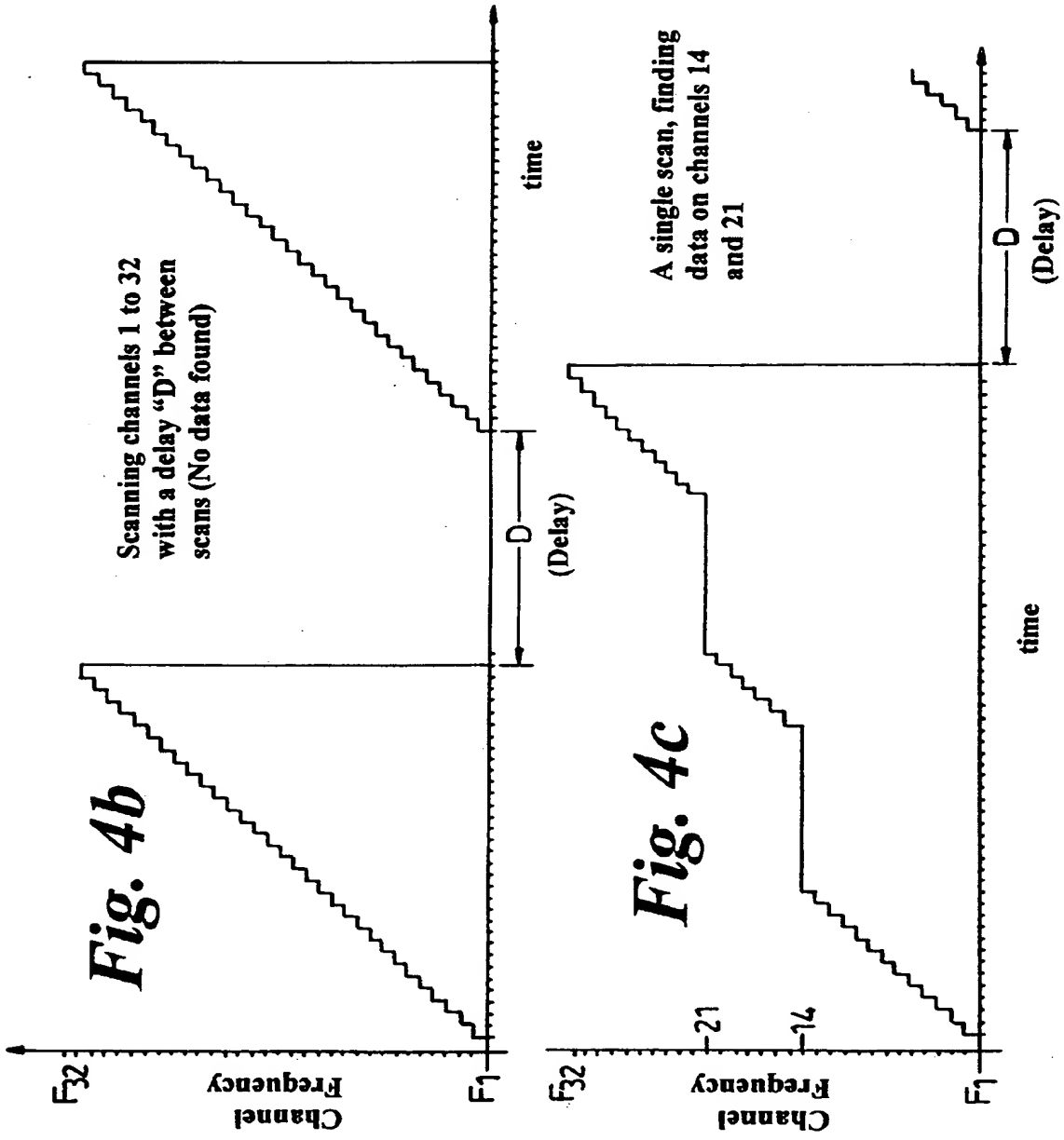

Channel Frequency
F32
F1
time
D
(Delay)
Scanning channels 1 to 32 with a delay "D" between scans (No data found)
A single scan, finding data on channels 14 and 21
21
14

Fig. 4b

Fig. 4c

A Security System

This invention relates to security systems and in particular to a security system suitable for use in a vehicle. The security system is of the type comprising a transmitter which is portable and a receiver which is included in or on the protected unit and which communicate with each other using electromagnetic signals, usually transmitted at radio frequencies.

Such systems can suffer from interference from other sources of radiation which appears around the operating frequency of the system and can prevent its proper operation. It is also known for car thieves to try and cause the remote transmitter to transmit a signal when it is not near the vehicle so that they can try to relay that signal to the vehicle in the hope that the relayed signal will operate the security system.

One proposal to reduce the effects of interference in this type of system is disclosed in US 4,751,396. In this system, a transmitter is arranged to send a signal at a single frequency and is matched to a receiver using both the baud rate of the signal and a code included in the transmission.

Another proposal to reduce the effects of interference in this type of system is disclosed in GB 2311155. In this system the remote transmitter sends its signal at two frequencies and uses frequency key shifting (FSK). Verification that an uncorrupted signal has been received is achieved by

comparing a coded portion of the received signal with a codeword stored in the receiver. It is a problem with this system that, if interference is suffered at both the transmitted frequencies, then the chances of either transmission being received are reduced.

The use of FSK necessitates the selection of frequencies which are quite close to each other, for example they are typically spaced apart by about 30 kHz. The narrow spacing is necessary to prevent unwanted harmonics causing interference to other systems.

The use of FSK does not significantly improve security over a system which transmits at only a single frequency because potential thieves merely have to include an FSK demodulator in their code grabbing apparatus. In this manner, the communications between the transmitter and receiver can be captured more or less as easily as if they were to be transmitted on only a single frequency.

It is an object of this invention to provide an improved security system.

According to the invention there is provided security system comprising a remote transponder arranged to communicate with a receiver which is associated with a security controller, the remote transponder being arranged in use to transmit a security signal in at least one channel of a

predetermined range of channels, the receiver being arranged in use to receive signals in any of said range of channels and the security controller being arranged in use to respond to the receipt of a said security signal by the receiver by performing a security function, wherein the receiver is arranged in use to scan said range of channels so as to determine in which channel or channels the security signal has been transmitted.

The receiver may be arranged to scan said range of channels by tuning itself to each of the channels and remaining tuned thereto for long enough to detect whether or not data is being transmitted in the channel which is being scanned.

The receiver may be arranged to abandon the scanning of a channel if it does not detect the transmission of data in that channel.

The receiver may be arranged to use an automatic frequency control (AFC) process to substantially centre itself onto data being transmitted in a channel which is being scanned.

The receiver may be arranged to remain tuned to a channel in which data has been detected until it determines whether or not the detected data comprises a plausible security signal.

The receiver, if it determines the detected data comprises a plausible security signal, may be arranged to remain tuned to that detected data until the security signal has been received.

The receiver may be arranged to abandon the scanning of a particular channel in which a plausible security signal was detected if that security signal becomes implausible.

The receiver may be arranged to continue its scanning of the channels after receiving the security signal in any one of the channels or after abandoning the scanning of any one of the channels.

The receiver may be arranged to remain tuned to a further one of the channels if data is detected in that further channel and to remain tuned thereto for long enough to determine if the data detected in that further channel comprises a plausible security signal, whereby, if the security signal is transmitted in a plurality of channels, the receiver can determine in which one or more of the channels the security signal is or was capable of detection and can provide to the security controller any such security signal which is received and an indication of the channel or channels in which the security signal was received.

The receiver may be arranged to remain tuned to a channel in which data is detected until the expiry of a predetermined time period, the expiry of which time period without the determination of the presence of plausible data being indicative that the detected data does not comprise or no longer comprises a plausible security signal.

The receiver may be arranged to increment a counter for a channel if it determines that the detected data in that channel does not comprise a plausible security signal.

The receiver may be arranged to increment a counter for a channel if the detected data in that channel over-runs or if it under-runs a plausible security signal. The counter may be incremented by a different amount for an over-run than for an under-run.

The receiver may be arranged to reduce the sensitivity of its reception for a channel if the counter exceeds a predetermined value and the sensitivity may be reduced in predetermined stages which may comprise one or more of 4, 8, and 12 dB.

The receiver may be arranged to stop receiving in a channel if, despite the reduction or reductions in sensitivity, the detected data in that channel continues to be determined as implausible.

The counter for a channel may be decremented at, towards or after a scan through the range of channels. The counter may be decremented by a lower value at, towards or after the end of a scan than the counter would be incremented for an over-run or for an under-run during a scan, whereby the counter is arranged to adopt a fast-on but slow-off measure of data plausibility for a channel.

The receiver may be arranged to provide to the security controller a signal indicative of a channel in which a plausible security signal was received.

The security controller may be arranged to compare the channel in which a plausible security signal is first received with the channel in which a following transmission thereof is received and to determine, from the spacing between the channels in which the security signal is received, whether the security signal has been relayed using relaying means, or has suffered interference or has been corrupted.

The remote transponder may be arranged to transmit the security signal first in one of the channels and then in a further one or more than one of the channels and the channel or channels in which the security signal is transmitted may be preset in the remote transponder. The channel or channels may be preset by the resonant frequency of an associated

When the security signal is transmitted in a plurality of channels, the respective associated surface acoustic wave resonators may be connected in parallel and, each time the security signal is transmitted, a first one of the resonators may be turned on to cause the security signal to be transmitted in a channel associated with that resonator and that first resonator may then be turned off and the next one of the resonators may then be turned on to cause the same security signal to be transmitted in a channel associated with that next one of the resonators.

When the security signal is transmitted in a plurality of channels, the resonant frequencies of the surface acoustic wave resonators may be selected such that there is a predetermined frequency gap between the channels in which the security signal is transmitted.

The remote transponder may be arranged to indicate to the receiver in which one or more than one of the predetermined range of channels the security signal is to be transmitted.

The remote transponder may be arranged to send an indicating signal to the receiver, which indicating signal indicates the channel or channels in which the security signal is to be transmitted.

The security controller may be arranged to send a specifying signal to the remote transponder in which specifying signal the security controller is arranged to specify to the remote transponder the channel or channels in which the remote transponder is to transmit the security signal.

When the security signal is transmitted in a plurality of channels, the frequency of at least one of the at least two channels in which the remote transponder transmits its signals may be alterable between transmissions.

The frequencies of the channels comprising said predetermined range of channels may be pre-programmed into the remote transponder and into at least one of the receiver or the security controller.

The remote transponder may be arranged to transmit the security signal in more than two of said predetermined range of channels and the security controller may be arranged to respond to said security signal only if it is received by the receiver in at least two channels.

Said predetermined range of channels may be 32 or 10 in number.

The channels used for transmission of the security signal may be of substantially equal width. When the security signal is transmitted in two

or more channels, the channels used for transmission of the security signal may be spaced apart by at least one channel.

Said predetermined range of channels may have a bandwidth in the order of 480 kHz.

The security signal may be transmitted in two or more channels and the channels used for transmission of the security signal may be spaced apart by at least three channels.

Said predetermined range of channels may have a bandwidth in the order of 1 MHz.

The remote transponder may be arranged to transmit the security signal only in response to a request signal transmitted to it by a transmitting means. The request signal may be transmitted as a result of an action of a user of a vehicle, to which the system has been fitted, triggering the transmitting means. The transmitting means may be triggered by operation of an opening mechanism of a closure member of the vehicle. The receiver may be arranged, after completing a scan through said range of channels, to wait for a predetermined delay period before commencing another scan.

The invention also provides: a security controller for a security system according to the invention; a remote transponder for a security system according to the invention, the remote transponder being arranged to transmit the security signal first in one of the range of channels and then in at least a further one of the range of channels; and a vehicle including a security system according to the invention.

The invention also provides a method of controlling a security system, the system comprising a remote transponder arranged to communicate with a receiver which is associated with a security controller, the remote transponder being arranged in use to transmit a security signal in at least one channel of a predetermined range of channels, the receiver being arranged in use to receive signals in any of said range of channels and the security controller being arranged in use to respond to the receipt of a said security signal by the receiver by performing a security function, the method including scanning said range of channels so as to determine in which channel or channels the security signal has been transmitted.

The method may include scanning said range of channels by tuning the receiver to each of the channels and remaining tuned thereto for long enough to detect whether or not data is being transmitted in the channel which is being scanned.

The method may include abandoning the scanning of a channel if the receiver does not detect the transmission of data in that channel.

The method may include using an automatic frequency control (AFC) process to substantially centre the receiver onto data being transmitted in a channel which is being scanned.

The method may include remaining tuned to a channel in which data has been detected until determining whether or not the detected data comprises a plausible security signal.

The method may include remaining tuned, if the receiver determines that the detected data comprises a plausible security signal, to the detected data until the security signal has been received.

The method may include abandoning the scanning of a particular channel in which a plausible security signal was detected if that signal becomes implausible.

The method may include continuing to scan said range of channels after receiving the security signal in any one of the channels or after abandoning the scanning of any one of the channels.

The method may include keeping the receiver tuned to a further one of the channels if data is detected in that further channel and keeping the receiver tuned thereto for long enough to determine if the data detected in that further channel comprises a plausible security signal, whereby, if the security signal is transmitted in a plurality of channels, the method includes determining in which one or more of the channels the security signal is or was capable of detection and providing to the security controller any such security signal which is received and an indication of the channel or channels in which the security signal was received.

The method may include keeping the receiver tuned to a channel in which data is detected until the expiry of a predetermined time period, the expiry of which time period without determining the presence of plausible data indicating that the detected data does not comprise or no longer comprises a plausible security signal.

The method may include incrementing a counter for a channel if the receiver determines that the detected data in that channel does not comprise a plausible security signal.

The method may include incrementing a counter for a channel if the detected data in that channel over-runs or if it under-runs a plausible

security signal. The method may include incrementing the counter by a different amount for an over-run than for an under-run.

The method may include reducing the sensitivity of reception of the receiver for a channel if the counter exceeds a predetermined level.

The method may include reducing the sensitivity in predetermined stages. The method may include stopping the receiver from receiving in a channel if, despite reducing the sensitivity of the receiver, the detected data in that channel continues to be determined as implausible.

The method may include decrementing the counter for a channel at, towards or after a scan through the range of channels and may include decrementing the counter for a channel by a lower value at, towards or after the end of a scan than the counter would be incremented for an over-run or for an under-run during a scan, whereby the method may include the counter adopting a fast-on but slow-off measure of data plausibility for a channel.

The method may include providing the security controller with a signal indicative of a channel in which a plausible security signal was received.

The method may include comparing the channel in which a plausible security signal is first received with the channel in which a following transmission thereof is received and determining, from the spacing between the channels in which the security signal is received, whether the security signal has been relayed using a relaying means or has suffered interference or has been corrupted.

The method may include transmitting the security signal first in one of the channels and then in a further one or more than one of the channels.

The method may include indicating from the remote transponder to the receiver in which one or more than one of the predetermined range of channels the security signal is to be transmitted.

The method may include sending to the receiver from the remote transponder an indicating signal which indicates the channel or channels in which the security signal is to be transmitted.

The method may include sending a specifying signal to the remote transponder from the security controller, in which specifying signal the security controller specifies the channel or channels in which the remote transponder is to transmit the security signal.

The method may include when the security signal is transmitted in a plurality of channels, altering between transmissions of the security signal the frequency of at least one of the plurality of channels in which the remote transponder transmits the security signal.

The method may include transmitting the security signal in more than two of said predetermined range of channels and arranging the security controller to respond to the security signal only if it is received by the receiver in at least two channels.

The method may include when the security signal is transmitted in two or more channels, spacing apart the channels used for transmission of the security signal by at least one channel.

The method may include waiting for a predetermined delay period after completing a scan through said range of channels before commencing another scan.

Preferred embodiments of the invention will now be described by way of example only and with reference to the accompanying drawings, in which:

Figure 1 is a schematic view of a vehicle including a security system according to the invention;

Figure 2 is a flow chart of a method of operation of a remote transponder of the security system of Figure 1;

Figure 3 is a flow chart of a method of operation of a receiver of a security controller of Figure 1; and

Figures 4a to 4c are a graphical representation of part of the method of Figure 3.

Referring to the figures, a vehicle 10 comprises a security system which includes a security controller 12 which has associated with it a first transmitter / receiver unit 14 and which controls the operation of various items on the vehicle including the door locks and an engine imobiliser.

The security system also includes a remote transponder 16 which is portable and intended in use to be carried by a user. The transponder 16 includes a second transmitter / receiver unit 18 and an associated control circuit 20 and is arranged to communicate selectively with the security controller 12.

The vehicle 10 has a closure member operating mechanism in the form of a door handle 22 on the driver's door 24 which has a microswitch (not shown separately) in it to enable the controller 12 to detect when the door

handle 22 is operated to gain entry to the vehicle 10. The controller 12 reacts to operation of the door handle 22 by causing the first transmitter / receiver unit 14 to transmit a request signal to the remote transponder 16 as will be described below.

The transmitter / receiver units 14, 18 each have an operative bandwidth in the order of 480 kHz. This total operative band is divided into 32 frequency bands or channels, each about 15 kHz in width. The channels are adjacent to one another, are non-overlapping and are distinguishable from each other by their frequency of operation Fn. The channels rise in frequency from (n=1) to ($n=n_{max}$). In this embodiment, having 32 channels, n rises between successive channels from (n=1) to (n=32) evenly spaced across the total bandwidth of 480 kHz.

Each of the transmitter / receiver units 14, 18 is arranged such that it can transmit in each of the channels independently, receive signals in each of the channels, and distinguish between signals received in different channels. The control circuit 20 in the transponder 16 and the security controller 12 on the vehicle 10 control the timing and frequency of the transmissions and process the signals received by their respective receivers.

When a user approaches the vehicle 10 and lifts the door handle 22, the controller 12 causes the first transmitter / receiver unit 14 to transmit in

one of the channels a request signal, for example at 125 kHz, which requests that the transponder 16 send a coded security signal in response.

The transponder 16 is arranged to respond to the request signal by transmitting in two of the channels and the response comprises a coded security signal which is transmitted first in one channel and then in a second one. Using successive transmissions means that harmonics are not generated and the problems associated with frequency shift keying (FSK) do not occur, which in turn means that channel spacing is not restricted as it might be if FSK were to be used.

The channels used for the response are fixed in the transponder 16 during manufacture by the inclusion of surface acoustic wave resonators (SAWs) (not shown separately) in the control circuit 20. The SAWs are connected in parallel and arranged to be capable of being switched on independently and selectively.

To send the response, one of the SAWs is turned on using a pin diode and this results in the security signal being transmitted in the channel in which that particular SAW's resonant frequency falls. This SAW is then turned off and the other SAW is turned on, again using a pin diode. The security signal is then transmitted in the channel in which the resonant frequency of the second SAW falls. The second SAW is then turned off and

transmission of the response for that receipt of the request signal is complete.

The SAWs are selected such that their nominal resonant frequencies result in the transmission channels of the response have a spacing of at least three or four channels between them, or more preferably a spacing of at least 100 kHz.

The SAWs' frequencies cannot be guaranteed as fixed, as their nominal resonant frequency will drift with time and variations in temperature. Because of this, it is not possible to specify with absolute certainty which of the channels will be used to transmit the response and the receiver / transmitter unit 14 must therefore scan all the channels to find the one or more than one in which the security signal can be detected.

To scan across all the channels Fn to Fn_{max}, the transmitter / receiver unit 14 scans the channels by tuning itself to each one in turn and waiting in each channel Fn long enough to detect whether there is data present in an expected format, which can then be analysed to determine if it comprises a security signal. One example of data in an expected format can be achieved by providing the security signal with a long preamble of logic "1" bits so as to make it easy to find and then keeping the receiver of the

transmitter / receiver unit 14 tuned into each channel long enough to detect a recognisable portion of this preamble.

When the transmitter / receiver unit 14 has found a channel in which data appears to be present, it uses an automatic frequency control process to centre itself onto that detected data and stays tuned to it until the security signal is complete and plausible, until the data becomes implausible (e.g. by over-running or under-running), or until a time-out has expired.

The scanning operation is best understood in greater detail with particular reference to Figure 3 and Figures 4a to 4c.

In Figure 4a, the basic scanning operation can be observed but without the detection of data in any of the channels. In the basic scanning operation, the transmitter / receiver unit 14 is constantly scanning through all 32 channels in succession looking for the security signal. Each scan starts at the channel having the lowest frequency Fn (where n=1). If no data is detected, the scan moves onto the next channel F(n=n+1). If the transmitter / receiver unit 14 scans through all 32 of the channels (Fn to Fn_{max}) without detecting data, the scan starts again at F(n=1). In any case, once Fn_{max} has been scanned, n is set back to 1, so that the next scan is ready to start.

With particular reference to Figures 3 and 4b, a delay period D is optionally included between scans so as to reduce power consumption. The delay period D is preferably set at a length which is not long enough to cause inconvenience to a user who might have to wait for the delay D to end before the scanning could start. A suitable and convenient delay D might be found to exist in the range of 32 to 256 ms.

In Figure 4c, only one scan from either of Figures 4a or 4b is shown, the transmitter / receiver unit 14 having transmitted the security signal in two channels, first in F(n=14) and then in F(n=21) in accordance with the flow chart of Figure 2. Data can be seen to have been detected in channels 14 and 21 and when such detected data is determined within the receiver of the transmitter / receiver 14 to be a plausible security signal, it is passed to the remainder of the security controller 12 for implementation as a predetermined security function.

When data has been detected in the expected format in any particular channel, found to be plausible and passed to the remainder of the security controller, the data output to the security controller from the transmitter / receiver 14 is disabled and the next channel in succession is scanned, in search of a repeat transmission (such as the one found in the above example in channel 21).

If data detected in a channel under-runs or over-runs a plausible security signal, that event is noted by incrementing by a constant N_{und} or N_{over} respectively a counter value for a register associated with that channel. A different constant is used when incrementing the counter for each of an under-run and an over-run. The constants are not equal and the constant used for an over-run is the greater because an over-run usually indicates that the signal has been subjected to interference.

If the counter value for a given channel reaches one of a series of thresholds, the transmitter / receiver unit 14 is arranged to assume that there is an interfering signal which is causing it to waste time looking for the security signal in that channel at that time. When this happens, the transmitter / receiver unit 14 first reduces the sensitivity of the receiver of its transmitter / receiver unit 14 for the affected channel and does so in graduated steps (for example 4, 8, 12 dB).

If the counter value exceeds a preset maximum despite the reduction or reductions in sensitivity, the transmitter / receiver unit 14 will finally shut down for that channel or channels which is / are then by-passed completely until the counter has been cleared as outlined below.

At, towards or after the end of each scan, the counter value for the counter of each channel is decremented. The counter is decremented by a

smaller amount than the value of either N_{und} or N_{over}. For example, N_{und} may be 4, N_{over} may be 5 and the counter decremented at, towards or after each scan by 1. In this manner, the counter adopts a "fast-on" but "slow-off" measure of data plausibility for each channel. This feature means that it takes 4 or 5 scans, without either under-running or over-running, to clear the counter for a channel for each under-run or over-run as the case may be of data in that channel.

If a channel is being by-passed because its counter has exceeded a predetermined threshold, which might for this example be between 12 and 16, the counter is still decremented by 1 at, towards or after each scan along with the counters for all the other channels. In this manner, any affected channel is only ignored for a predetermined number of scans, e.g. 12 to 16, and the system can thus accommodate transient interference in any one or more than one of the channels.

A different way of deciding that the data is implausible would be to stay centred onto a string of detected data for a predetermined time period, the expiry of which could be pre-programmed into the receiver of the transmitter / receiver unit 14 as indicative that the data being received does not comprise a plausible security signal. For example, such a time-out could be set to correspond to an over-run condition.

When the transmitter / receiver unit 14 has detected a plausible security signal and passed it on to the remainder of the security controller 12, it is followed by a message which identifies the channel in which the security signal was detected. The security controller 12 uses this information about that channel to make a comparison with the other channel (if any) in which the security signal was detected and to judge whether the channel spacing is sufficient to indicate a valid response or one which has suffered interference. If the security signal is detected in only one channel, then information about which channel that might be is of limited use, except for example to verify that the security signal was detected in a valid channel.

By sending out the security signal on first one channel and then on another one, instead of for example both at the same time, the likelihood of generating undesirable harmonics is significantly reduced.

In a second embodiment of the invention, the response comprises the security signal sent in only one channel and thus saves the cost of the second SAW. Such an embodiment is useful in a market where there is a reduced risk of vehicle theft. In most cases, however, it is preferred to transmit the security signal in two or more channels as described in the first embodiment so as to provide protection against interference in any one channel.

The use of a bandwidth of about 480 kHz, still around a central frequency of about 433 MHz and which is divided into 32 channels each being about 15 kHz wide, could be applied to other embodiments of the invention. Embodiments in which the security signal is transmitted on more than one channel have the advantage that a channel spacing of three or four can be used to transmit the security signals closer to each other than would be easy to detect using a commercially available UHF receiver of reasonable cost and which might have a bandwidth of, for example, 500 kHz.

In this manner, a thief trying to use a code scanner based on such technology would find it more difficult to collect the security signal and to retransmit it. The security signals would appear as a single signal and that is what would be retransmitted after capture or relaying. Because the retransmitted or relayed signal is not two signals of narrow bandwidth which are close to each other, the security controller 12 could determine that such a signal was false or corrupted. Channel spacing of three or four also provides sufficient spacing to take account of the tolerances and drift of any SAW used.

In a third embodiment of the invention, the channels used for transmitting the security signal can be altered by the remote transponder 16 between transmissions of the response and the security controller 12

sends a specifying signal to the remote transponder 16 in order to specify in which one or more of the channels the transponder 16 is to send the security signal.

In this embodiment, the controller 12 is preferably arranged to select a different pair of channels for each response, i.e. each time the door handle 22 is lifted. This is achieved by an algorithm in the controller 12 (e.g. a random number generator which operates in the range of 1 to 32) and makes it harder for a thief to anticipate which channels will be used next.

In a fourth embodiment of the invention, the frequency of the response can also be altered under the control of the remote transponder 16. Upon receipt of a request signal, the remote transponder 16 sends an indicating signal to the transmitter / receiver 14 in order to specify in which one or more of the channels the security signal is to be sent.

Interference or corruption, for example from amateur radio transmissions, is usually limited to a relatively narrow bandwidth of about 50 kHz. Therefore, provided the channels chosen or specified for the third and fourth embodiments are not adjacent, the security signal will still be received and plausible in at least one channel even if the frequency of the interference falls within one of the channels.

The spacing of the channels in this case is such that they are always spaced apart by at least one channel so that a 50 kHz signal cannot interfere with both channels. If a different bandwidth or a different number of channels are used, the channel spacing would merely be altered to suit the new bandwidth or number of channels so as to avoid interference from this or another interfering signal.

In a fifth embodiment of the invention, the transponder 16 is arranged to transmit a signal in each of three or more of the channels. The receiver is arranged to scan all of the channels and to respond by producing a re-mobilisation signal if it receives the signal in at least any two of the channels. In this way the exact frequency of the transmission is not critical, the only requirement being that two signals in different channels are received. This makes the fluctuations in frequency which can result from temperature changes less harmful to the system, whilst allowing the system to operate if there is interference in one of the channels.

The transmitter / receiver unit 14 does not need to be a separate unit and could be included in the security controller 12 in this and in any other embodiment.

In each embodiment, if a thief tries to trigger the transponder 16 when it is remote from the vehicle and tries to relay the transmitted signal to the

vehicle 10, he will encounter at least two problems. Firstly, he is unlikely to be able to transmit a signal to the transponder 16 which is in the correct channel to produce a response. Secondly, if he does produce a response, he is unlikely to be able to detect accurately enough in which channel or channels the security signal is being transmitted to be able to relay it correctly.

The frequency band should not be considered as limited to 480 kHz in any embodiment. For example, it may be possible to use a bandwidth of 1 MHz and to divide it into 10 channels. This would provide a channel bandwidth of 100 kHz and a channel spacing of only one channel would be adequate to substantially reduce the likelihood of interference. In addition, the cost of equipment which can distinguish between frequency bands of the order of 100 kHz is currently high and is not likely to be in the possession of most car thieves.

CLAIMS

1. A security system comprising a remote transponder arranged to communicate with a receiver which is associated with a security controller, the remote transponder being arranged in use to transmit a security signal in at least one channel of a predetermined range of channels, the receiver being arranged in use to receive signals in any of said range of channels and the security controller being arranged in use to respond to the receipt of a said security signal by the receiver by performing a security function, wherein the receiver is arranged in use to scan said range of channels so as to determine in which channel or channels the security signal has been transmitted.

2. A security system according to Claim 1, wherein the receiver is arranged to scan said range of channels by tuning itself to each of the channels and remaining tuned thereto for long enough to detect whether or not data is being transmitted in the channel which is being scanned.

3. A security system according to Claim 2, wherein the receiver is arranged to abandon the scanning of a channel if it does not detect the transmission of data in that channel.

4. A security system according to Claim 2 or Claim 3, wherein the receiver is arranged to use an automatic frequency control (AFC) process to substantially centre itself onto data being transmitted in a channel which is being scanned.

5. A security system according to any one of Claims 2 to 4, wherein the receiver is arranged to remain tuned to a channel in which data has been detected until it determines whether or not the detected data comprises a plausible security signal.

6. A security system according to Claim 5, wherein the receiver, if it determines the detected data comprises a plausible security signal, is arranged to remain tuned to that detected data until the security signal has been received.

7. A security system according to Claim 6, wherein the receiver is arranged to abandon the scanning of a particular channel in which a plausible security signal was detected if that security signal becomes implausible.

8. A security system according to any preceding claim, wherein the receiver is arranged to continue its scanning of the channels after

receiving the security signal in any one of the channels or after abandoning the scanning of any one of the channels.

9. A security system according to any one of Claims 2 to 8, wherein the receiver is arranged to remain tuned to a further one of the channels if data is detected in that further channel and to remain tuned thereto for long enough to determine if the data detected in that further channel comprises a plausible security signal, whereby, if the security signal is transmitted in a plurality of channels, the receiver can determine in which one or more of the channels the security signal is or was capable of detection and can provide to the security controller any such security signal which is received and an indication of the channel or channels in which the security signal was received.

10. A security system according to any one of Claims 5 to 9, wherein the receiver is arranged to remain tuned to a channel in which data is detected until the expiry of a predetermined time period, the expiry of which time period without the determination of the presence of plausible data being indicative that the detected data does not comprise or no longer comprises a plausible security signal.

11. A security system according to any one of Claims 5 to 10, wherein the receiver is arranged to increment a counter for a channel if it

determines that the detected data in that channel does not comprise a plausible security signal.

12. A security system according to any one of Claims 5 to 11, wherein the receiver is arranged to increment a counter for a channel if the detected data in that channel over-runs or if it under-runs a plausible security signal.

13. A security system according to Claim 12, wherein the counter is incremented by a different amount for an over-run than for an under-run.

14. A security system according to any one of Claims 11 to 13, wherein the receiver is arranged to reduce the sensitivity of its reception for a channel if the counter exceeds a predetermined value.

15. A security system according to Claim 14, wherein the sensitivity is reduced in predetermined stages.

16. A security system according to Claim 15, wherein the predetermined stages comprise one or more of 4, 8, and 12 dB.

17. A security system according to any one of Claims 11 to 16, wherein the receiver is arranged to stop receiving in a channel if, despite the

reduction or reductions in sensitivity, the detected data in that channel continues to be determined as implausible.

18. A security system according to any one of Claims 11 to 17, wherein the counter for a channel is decremented at, towards or after a scan through the range of channels.

19. A security system according to Claim 18, wherein the counter for a channel is decremented by a lower value at, towards or after the end of a scan than the counter would be incremented for an over-run or for an under-run during a scan, whereby the counter is arranged to adopt a fast-on but slow-off measure of data plausibility for a channel.

20 A security system according to any one of Claims 5 to 19, wherein the receiver is arranged to provide to the security controller a signal indicative of a channel in which a plausible security signal was received.

21. A security system according to Claim 20, wherein the security controller is arranged to compare the channel in which a plausible security signal is first received with the channel in which a following transmission thereof is received and to determine, from the spacing between the channels in which the security signal is received, whether

the security signal has been relayed using relaying means, or has suffered interference or has been corrupted.

22. A security system according to any preceding claim, wherein the remote transponder is arranged to transmit the security signal first in one of the channels and then in a further one or more than one of the channels.

23. A security system according to any preceding claim, wherein the channel or channels in which the security signal is transmitted is or are preset in the remote transponder.

24. A security system according to Claim 23, wherein the channel or channels is or are preset by the resonant frequency of an associated respective surface acoustic wave resonator (SAW resonator).

25. A security system according to Claim 24, wherein, when the security signal is transmitted in a plurality of channels, the respective associated surface acoustic wave resonators are connected in parallel and, each time the security signal is transmitted, a first one of the resonators is turned on to cause the security signal to be transmitted in a channel associated with that resonator and that first resonator is then turned off and the next one of the resonators is then turned on to cause

the same security signal to be transmitted in a channel associated with that next one of the resonators.

26. A security system according to Claim 24 or Claim 25, wherein, when the security signal is transmitted in a plurality of channels, the resonant frequencies of the surface acoustic wave resonators are selected such that there is a predetermined frequency gap between the channels in which the security signal is transmitted.

27. A security system according to Claim 1, wherein the remote transponder is arranged to indicate to the receiver in which one or more than one of the predetermined range of channels the security signal is to be transmitted.

28. A security system according to Claim 27, wherein the remote transponder is arranged to send an indicating signal to the receiver, which indicating signal indicates the channel or channels in which the security signal is to be transmitted.

29. A security system according to Claim 1, wherein the security controller is arranged to send a specifying signal to the remote transponder in which specifying signal the security controller is

arranged to specify to the remote transponder the channel or channels in which the remote transponder is to transmit the security signal.

30. A security system according to any preceding claim, wherein, when the security signal is transmitted in a plurality of channels, the frequency of at least one of the at least two channels in which the remote transponder transmits its signals is alterable between transmissions.

31. A security system according to any preceding claim, wherein the frequencies of the channels comprising said predetermined range of channels are pre-programmed into the remote transponder and into at least one of the receiver or the security controller.

32. A security system according to any preceding claim, wherein the remote transponder is arranged to transmit the security signal in more than two of said predetermined range of channels and wherein the security controller is arranged to respond to said security signal only if it is received by the receiver in at least two channels.

33. A security system according to any preceding claim, said predetermined range of channels being 32 in number.

34. A security system according to any one of Claims 1 to 32, said predetermined range of channels being 10 in number.

35. A security system according to any preceding claim, wherein the channels used for transmission of the security signal are of substantially equal width.

36. A security system according to any preceding claim, wherein, when the security signal is transmitted in two or more channels, the channels used for transmission of the security signal are spaced apart by at least one channel.

37. A security system according to any preceding claim, wherein said predetermined range of channels has a bandwidth in the order of 480 kHz.

38. A security system according to Claim 37, wherein the security signal is transmitted in two or more channels and the channels used for transmission of the security signal are spaced apart by at least three channels.

39. A security system according to any one of Claims 1 to 36, wherein said predetermined range of channels has a bandwidth in the order of 1 MHz.

40. A security system according to any preceding claim, wherein the remote transponder is arranged to transmit the security signal only in response to a request signal transmitted to it by a transmitting means.

41. A security system according to Claim 40, wherein the request signal is transmitted as a result of an action of a user of a vehicle, to which the system has been fitted, triggering the transmitting means.

42. A security system according to Claim 41, the transmitting means being triggered by operation of an opening mechanism of a closure member of the vehicle.

43. A security system according to any preceding claim, wherein the receiver is arranged, after completing a scan through said range of channels, to wait for a predetermined delay period before commencing another scan.

44. A security system substantially as described herein with reference to the accompanying drawings.

45. A security controller for a security system according to any preceding claim.

46. A remote transponder for a security system according to any one of Claims 1 to 44, the remote transponder being arranged to transmit the security signal first in one of the range of channels and then in at least a further one of the range of channels.

47. A vehicle including a security system according to any one of Claims 1 to 44.

48. A method of controlling a security system, the system comprising a remote transponder arranged to communicate with a receiver which is associated with a security controller, the remote transponder being arranged in use to transmit a security signal in at least one channel of a predetermined range of channels, the receiver being arranged in use to receive signals in any of said range of channels and the security controller being arranged in use to respond to the receipt of a said security signal by the receiver by performing a security function, the method including scanning said range of channels so as to determine in which channel or channels the security signal has been transmitted.

49. A method according to Claim 48, including scanning said range of channels by tuning the receiver to each of the channels and remaining tuned thereto for long enough to detect whether or not data is being transmitted in the channel which is being scanned.

50. A method according to claim 49, including abandoning the scanning of a channel if the receiver does not detect the transmission of data in that channel.

51. A method according to Claim 49 or Claim 50, including using an automatic frequency control (AFC) process to substantially centre the receiver onto data being transmitted in a channel which is being scanned.

52. A method according to any one of Claims 49 to 51, including remaining tuned to a channel in which data has been detected until determining whether or not the detected data comprises a plausible security signal.

53. A method according to Claim 53, including remaining tuned, if the receiver determines that the detected data comprises a plausible security signal, to the detected data until the security signal has been received.

54. A method according to Claim 53, including abandoning the scanning of a particular channel in which a plausible security signal was detected if that signal becomes implausible.

55. A method according to Claim 54, including continuing to scan said range of channels after receiving the security signal in any one of the channels or after abandoning the scanning of any one of the channels.

56. A method according to any one of Claims 49 to 55, including keeping the receiver tuned to a further one of the channels if data is detected in that further channel and keeping the receiver tuned thereto for long enough to determine if the data detected in that further channel comprises a plausible security signal, whereby, if the security signal is transmitted in a plurality of channels, the method includes determining in which one or more of the channels the security signal is or was capable of detection and providing to the security controller any such security signal which is received and an indication of the channel or channels in which the security signal was received.

57. A method according to any one of Claims 52 to 56 including keeping the receiver tuned to a channel in which data is detected until the expiry of a predetermined time period, the expiry of which time period without determining the presence of plausible data indicating that the

detected data does not comprise or no longer comprises a plausible security signal.

58. A method according to any one of Claims 52 to 57 including incrementing a counter for a channel if the receiver determines that the detected data in that channel does not comprise a plausible security signal.

59. A method according to any one of Claims 52 to 58, including incrementing a counter for a channel if the detected data in that channel over-runs or if it under-runs a plausible security signal.

60. A method according to Claim 59, including incrementing the counter by a different amount for an over-run than for an under-run.

61. A method according to any one of Claims 58 to 60, including reducing the sensitivity of reception of the receiver for a channel if the counter exceeds a predetermined level.

62. A method according to Claim 61, including reducing the sensitivity in predetermined stages.

63. A method according to any one of Claims 58 to 62, including stopping the receiver from receiving in a channel if, despite reducing

the sensitivity of the receiver, the detected data in that channel continues to be determined as implausible.

64. A method according to any one of Claims 58 to 63, including decrementing the counter for a channel at, towards or after a scan through the range of channels.

65. A method according to Claim 64, including decrementing the counter for a channel by a lower value at, towards or after the end of a scan than the counter would be incremented for an over-run or for an under-run during a scan, whereby the method includes the counter adopting a fast-on but slow-off measure of data plausibility for a channel.

66. A method according to any one of Claims 52 to 65, including providing the security controller with a signal indicative of a channel in which a plausible security signal was received.

67. A method according to Claim 65, including comparing the channel in which a plausible security signal is first received with the channel in which a following transmission thereof is received and determining, from the spacing between the channels in which the security signal is received, whether the security signal has been relayed using a relaying means or has suffered interference or has been corrupted.

68. A method according to any one of Claims 48 to 67, including transmitting the security signal first in one of the channels and then in a further one or more than one of the channels.

69. A method according to Claim 48, including indicating from the remote transponder to the receiver in which one or more than one of the predetermined range of channels the security signal is to be transmitted.

70. A method according to Claim 69, including sending to the receiver from the remote transponder an indicating signal which indicates the channel or channels in which the security signal is to be transmitted.

71. A method according to Claim 48, including sending a specifying signal to the remote transponder from the security controller, in which specifying signal the security controller specifies the channel or channels in which the remote transponder is to transmit the security signal.

72. A method according to any one of Claims 48 to 71, including, when the security signal is transmitted in a plurality of channels, altering between transmissions of the security signal the frequency of at least

one of the plurality of channels in which the remote transponder transmits the security signal.

73. A method according to any one of Claims 48 to 72, including transmitting the security signal in more than two of said predetermined range of channels and arranging the security controller to respond to the security signal only if it is received by the receiver in at least two channels.

74. A method according to any one of Claims 48 to 73, including, when the security signal is transmitted in two or more channels, spacing apart the channels used for transmission of the security signal by at least one channel.

75. A method according to any one of Claims 48 to 74, including waiting for a predetermined delay period after completing a scan through said range of channels before commencing another scan.

76. A method substantially as described herein with reference to the accompanying drawings.

The Patent Office

46

Application No:	GB 9827361.8	**Examiner:**	Mike Davis
Claims searched:	1-44,47-76	**Date of search:**	25 January 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4H (HRCE, HRCM, HRCS, HTG)

Int Cl (Ed.6): B60R, E05B, G07C

Other:

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A	GB 2311155 A	(SIEMENS) eg abstract	-
X	US 4209783	(OHYAMA ET AL) eg abstract	1,48 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.